JOURNAL OF ALGEBRA 9, 451–477 (1968)

Subfields of Division Rings, I*

MURRAY M. SCHACHER

Department of Mathematics, Yale University, New Haven, Connecticut 06520

Communicated by I. N. Herstein

Received December 19, 1967

1. PRELIMINARIES

The theory developed in this paper arises from the following question: Given a field k and an irreducible polynomial f over k, does there exist a finite-dimensional central division algebra over k containing a root of f? For the most part we will restrict k to be an algebraic number field, although many of the results here apply to all the global fields of class field theory. By a global field we mean either an algebraic number field or a function field in one variable over a finite field. If the polynomial f gives rise to a Galois extension of k we will be especially interested in the significance of the Galois group. The next two definitions provide the fundamental notions in this context.

DEFINITION. If k is a field and L a finite extension of k, then L is *k-adequate* $\Leftrightarrow$ there is a division ring D central over k containing L as a maximal commutative subfield. Otherwise L is *k-deficient*.

DEFINITION. A finite group G is *k-admissible* $\Leftrightarrow$ there is a Galois extension L of k with $G = G(L/k)$, the Galois group of L over k, and L is k-adequate.

A division ring D which is finite-dimensional over its center k will be called a k-division ring. By Wedderburn's theorem $[D : k] = n^2$, the dimension of D over k is a square. The integer n is called the degree of D. Let m be the exponent of D— the order of D in $B(k)$, the Brauer group of k. We will say k is stable if $m = n$ for every k-division ring D. It is well known that global fields are stable.

The famous theorem of Albert, Brauer, Hasse and Noether states that any k-division ring over a global field k has a maximal subfield which is a

* Part of this work was submitted for the author's doctoral dissertation at the University of Chicago. The author was supported during much of this research by the Army Research Office (AROD) grant to the University of Chicago.

cyclic extension of k. However, this characterization is too weak for our purposes; it says nothing about what other maximal subfields are possible, and the proof itself shows there are infinitely many nonisomorphic choices for the cyclic maximal subfield. We explore these simultaneity questions a little further in Section 5.

If L is a finite extension field of k, we denote by $[L : k]$ the dimension of L over k. The subgroup of $B(k)$ consisting of elements split by L will be written $B(L/k)$. A tower of three fields $k \subset L \subset M$ gives rise to an exact sequence:

$$0 \to B(L/k) \to B(M/k) \xrightarrow{j} B(M/L) \tag{1.1}$$

where j in (1.1) is induced by $A \rightsquigarrow A \otimes_k L$ for A a central simple k-algebra split by M.

If L is a Galois extension of k, $G = G(L/k)$, and L^* the nonzero elements of L, then $B(L/k) \cong H^2(G, L^*)$, the ordinary second cohomology group of G with coefficients in L^*.

2. Global Fields

Suppose now k is a global field and L a finite extension. Our first task is to reformulate the notion of adequacy in terms of $[L : k]$ and $B(L/k)$.

Proposition 2.1. *If k is stable, then a finite extension L is k-adequate $\Leftrightarrow$ $B(L/k)$ has an element of order $[L : k]$.*

Proof. If L is k-adequate, then any k-division ring D containing L as maximal subfield is in $B(L/k)$ and has order $[L : k]$. Let $x \in B(L/k)$ have order $n = [L : k]$. Then some central simple algebra A in the class of x contains L as a maximal subfield. Let D be the constituent division ring of A. Since L is a maximal subfield of A, $[A : k] = n^2$. But $[D : k] = n^2$ since x has order n and k is stable. Thus $A = D$, and L is k-adequate.

At first glance our definition of adequacy is the wrong one for the problem we have posed. There is no reason why a k-division ring D with a root α of an irreducible polynomial f over k should contain $k(\alpha)$ as a maximal subfield. The next proposition shows that our definition is the right one at least for stable fields; the condition of maximality can be eliminated if k is stable.

Proposition 2.2. *Let k be stable and L a finite extension of k. Then L is k-adequate $\Leftrightarrow$ L is contained in a k-division ring.*

Proof. Suppose $k \subset L \subset D$, D a k-division ring. Imbed L in a subfield M of D which is maximal. By definition, M is k-adequate. Let $[M : L] = m$ and

$[L : k] = n$. We know $B(M/k)$ has an element x of order mn. In the exact sequence

$$0 \to B(L/k) \to B(M/k) \xrightarrow{j} B(M/L)$$

it is clear that $j(mx) = 0$, and so $mx \in B(L/k)$. But mx has order n; by Proposition 2.1 it follows that L is k-adequate.

COROLLARY 2.3. *If k is a stable field, then any subfield of a k-adequate extension is k-adequate.*

COROLLARY 2.4. *If k is stable, then any separable extension of k is k-adequate if its normal closure is.*

We shall see in the sequel that the converse of Corollary 2.4 is false.

From this point forth all fields involved will be global fields. We take as known the standard facts about valuations on global fields; they will alternately be called primes, prime spots, or spots. A local field is the completion of a global field k at a prime spot $\mathfrak{p}$, written $k_\mathfrak{p}$. We often call $k_\mathfrak{p}$ the localization at $\mathfrak{p}$, and the set of all $k_\mathfrak{p}$ the localizations of k. A local field of characteristic 0 is simply a finite extension of the p-adic field Q_p.

Our basic set-up is as follows: L is a finite Galois extension of the global field k, $G = G(L/k)$, and $[L : k] = n$. We have verified that L is k-adequate if and only if $H^2(G, L^*)$ has an element of order n. By class field theory:

$$H^2(G, L^*) \subset \sum_{\mathfrak{p}} H^2(G_\mathfrak{p}, L_\mathfrak{p}^*) \qquad \text{(direct sum)} \tag{2.1}$$

where $\mathfrak{p}$ runs over the prime spots of k, $G_\mathfrak{p}$ is the decomposition group at $\mathfrak{p}$, a subgroup of $G, L_\mathfrak{p}$ any of the isomorphic local extensions of $k_\mathfrak{p}$, and $G_\mathfrak{p} = G(L_\mathfrak{p}/k_\mathfrak{p})$. Each $H^2(G_\mathfrak{p}, L_\mathfrak{p}^*)$ of (2.1) is isomorphic by an invariant map $\mathrm{inv}_\mathfrak{p}$ to the unique subgroup of Q/Z, the additive group of rationals mod 1, of order $n_\mathfrak{p} = [L_\mathfrak{p} : k_\mathfrak{p}]$. $H^2(G, L^*)$ in (2.1) is that subgroup of the right-hand side composed of elements whose invariants have sum 0.

Suppose now $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime decomposition for n. Since $H^2(G, L^*)$ is an Abelian group, it is clear that $H^2(G, L^*)$ has an element of order n if and only if it has an element of order $p_i^{e_i}$ for each $i = 1, \ldots, r$. We will frequently write $H^2(G, L^*) = H^2(L/k)$, and $| G |$ for the order of G.

The following two propositions provide the essential tools of investigation.

PROPOSITION 2.5. *Let L be a Galois extension of k, $[L : k] = n$, and $G = G(L/k)$. Suppose p is a rational prime and r an integer. Then $H^2(L/k)$ has an element of order p^r if and only if $n_\mathfrak{p} = [L_\mathfrak{p} : k_\mathfrak{p}]$ is divisible by p^r for two different primes $\mathfrak{p}$ of k.*

Proof. Suppose $a \in H^2(L/k)$ has order p^r. We write $a = a_{\mathfrak{p}_1} + \cdots + a_{\mathfrak{p}_r}$ according to (2.1), where $a_{\mathfrak{p}_i} \in H^2(L_{\mathfrak{p}_i}/k_{\mathfrak{p}_i})$ for some primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of k. Then one of the $a_{\mathfrak{p}_i}$, say $a_{\mathfrak{p}_1}$, must have order divisible by p^r since the order of $a = p^r$. Clearly then $n_{\mathfrak{p}_1} = [L_{\mathfrak{p}_1} : k_{\mathfrak{p}_1}]$ has order divisible by p^r. But the condition that the sum of the invariants be 0 forces $n_{\mathfrak{p}_i} = [L_{\mathfrak{p}_i} : k_{\mathfrak{p}_i}]$ to be divisible by p^r for some other prime $\mathfrak{p}_i$ of k. These are the two required primes. Conversely, suppose $n_{\mathfrak{p}_1}$ and $n_{\mathfrak{p}_2}$ are divisible by p^r. Then we can find $a_{\mathfrak{p}_1} \in H^2(L_{\mathfrak{p}_1}/k_{\mathfrak{p}_1})$ and $a_{\mathfrak{p}_2} \in H^2(L_{\mathfrak{p}_2}/k_{\mathfrak{p}_2})$ with $a_{\mathfrak{p}_1}$ having invariant $1/p^r$ and $a_{\mathfrak{p}_2}$ having invariant $-1/p^r$. Then $a_{\mathfrak{p}_1} + a_{\mathfrak{p}_2}$ is the required element of $H^2(L/k)$ of order p^r.

The next proposition is essentially a reformulation of Proposition 2.5 in the special case when p^r is the order of a p-Sylow subgroup of G.

PROPOSITION 2.6. *Under the hypotheses of Proposition* 2.5, *if p^r is the highest power of p dividing n, then $H^2(L/k)$ has an element of order p^r if and only if $G_{\mathfrak{p}} = G(L_{\mathfrak{p}}/k_{\mathfrak{p}})$ contains a p-Sylow subgroup of G for two different primes $\mathfrak{p}$ of k.*

Proof. Since $G_{\mathfrak{p}}$ is a subgroup of G, $| G_{\mathfrak{p}} | = n_{\mathfrak{p}}$ is divisible by p^r if and only if a p-Sylow subgroup of $G_{\mathfrak{p}}$ is also a p-Sylow subgroup of G.

It is about time for an example of an extension which is not adequate: Let $k = Q$, the rational numbers, and L the splitting field of the polynomial $x^8 - 1$ over Q. Then $[L : Q] = 4$ and $G(L/Q] = Z_2 \oplus Z_2$. But $H^2(L/Q)$has no elements of order 4. For L is unramified at rational primes $p \neq 2$, hence $G_p = Z_2$ or is trivial (G_p must be cyclic). $G_2 = Z_2 \oplus Z_2$; the extension is totally ramified at the prime 2. Thus $n_p = 4$ only for $p = 2$; Proposition 2.5 shows $H^2(L/Q)$ has no element of order 4. By definition, L is Q-deficient. By Proposition 2.2 the splitting field of $x^m - 1$ is Q-deficient whenever $8 \mid m$.

It follows that L above is contained in no finite-dimensional divising ring with center Q. Restated, this says the following: Any division ring with center Q containing a root of $x^4 + 1$ is infinite-dimensional. The concluding remark of the example above shows the same result holds for $x^4 + 1$ replaced by the irreducible cyclotomic polynomial $\phi_m(x)$ where $8 \mid m$. We will find a plethora of such "distinguishing polynomials" in the sequel.

For G to be k-admissible it need not happen that every normal extension L with $G = G(L/k)$ be k-adequate; we insist only that there be one such. Hence the example above does not legislate that $Z_2 \oplus Z_2$ is not Q-admissible; the root field M of the polynomial $x^{12} - 1$ has the same Galois group and is Q-adequate.

We aim now for a theorem which characterizes which groups can be Galois groups of deficient extensions. The critical tool is the following lemma, which is stated without proof in [*3*]. A complete proof is offered by Georges Whaples in ([*14*], (241)).

LEMMA 2.7. (Whaples). *Suppose L is a Galois extension of the algebraic number field k with $G = G(L/k)$. Then there is a finite extension E of k such that $G = G(EL/E)$ and EL/E is unramified at every prime of k.*

DEFINITION. A finite group G is called totally-admissible if and only if for every pair of global fields L and k with L Galois over k and $G = G(L/k)$, it follows that L is k-adequate.

THEOREM 2.8. *G is totally-admissible if and only if every Sylow subgroup of G is cyclic.*

Proof. Sufficiency: By Lemma 2.7 we may assume that $G = G(L/k)$ with L/k Galois, L/k unramified, and L k-adequate. Then $G_{\mathfrak{p}}$ contains a given p-Sylow subgroup of G for two different primes $\mathfrak{p}$ of k. But $G_{\mathfrak{p}}$ must be cyclic since $\mathfrak{p}$ is unramified in L; arguing on each prime dividing the order of G we conclude that every Sylow subgroup is cyclic.

Necessity: Suppose p^r is the highest power of p dividing $|G|$. It is enough to show that $H^2(L/k)$ has an element of order p^r. Let P be a p-Sylow subgroup of G and $M =$ the fixed field of P in the Galois correspondence for L/k. Then $G(L/M) = P$. By Theorem 3 of [3], there are infinitely many primes of M which are inertial in L (i.e. unramified having a unique local extension). We select $\mathfrak{p}_1$ and $\mathfrak{p}_2$, two such so that their restrictions to k, q_1 and q_2, are unequal. Then

$$[L_{\mathfrak{p}_1} : M_{\mathfrak{p}_1}] = [L_{\mathfrak{p}_2} : M_{\mathfrak{p}_2}] = p^r. \qquad \text{For} \quad i = 1, 2$$

$$[L_{q_i} : k_{q_i}] = [L_{\mathfrak{p}_i} : M_{\mathfrak{p}_i}][M_{\mathfrak{p}_i} : k_{q_i}]$$

showing the local degree at q_i is divisible by p^r. Proposition 2.5 verifies $H^2(L/k)$ has an element of order p^r.

Remark 1. The proof of Theorem 2.9 actually yields this stronger result: If p^r is the highest power of p dividing $|G|$ and a p-Sylow subgroup of G is cyclic, then $H^2(L/k)$ has an element of order p^r.

Remark 2. Theorem 2.8 gives a partial converse to the celebrated theorem on rational division algebras; if L is a cyclic extension of an algebraic number field k, then L is a maximal subfield of a k-division ring D. The proof of Theorem 2.8 shows in fact that there are infinitely many nonisomorphic choices for D.

Remark 3. In particular, any group G which is totally admissible is solvable; in fact G has a normal series with each Sylow subgroup as factor group. By Theorem 2.8 and well-known properties of number fields we

conclude that any nonsolvable group occurs as a Galois group of a pair of algebraic number fields L, k with $G = G(L/k)$ and L k-deficient.

We can, in questions of admissibility, pass to subgroups, but only at the price of raising the base field.

PROPOSITION 2.9. *If L is k-adequate and M any intermediate field, $k \subset M \subset L$, then L is M-adequate. In particular, if L shows a finite group G to be k-admissible and M is the fixed field of a subgroup H of G in the Galois correspondence, then L shows H to be M-admissible.*

Proof. There is a k-division ring D with L as maximal subfield. Let $D_1 =$ centralizer of M in D. D_1 is a division ring which, by the double centralizer theorem, has center M. It is clear that L is a maximal subfield of D_1. But $G(L/M) = H$ implies H is M-admissible.

3. NUMBER THEORETIC RESULTS

In this section we investigate the Q-adequacy of the fields $Q(\sqrt{p}, \sqrt{q})$ where p and q are primes. Since quadratic extensions of Q are Q-adequate by Theorem 2.8, these fields represent in a sense the first level of difficulty. They all have dimension 4 over Q with Galois group $Z_2 \oplus Z_2$.

If p is an odd prime and n any integer prime to p, the Legendre symbol (n/p) is defined as follows:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is congruent to a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

It is well known that the Legendre symbol is multiplicative. The results of this section depend essentially on the law of quadratic reciprocity ([*13*], 7–3–3), which states

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{(p-1)/2} \\ \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8} \end{aligned} \tag{3.1}$$

For q an odd prime $\neq p$: $(p/q)(q/p) = (-1)^{[(p-1)/2 \cdot (q-1)/2]}$.

We begin with the easiest case, namely one of p or q equals 2.

THEOREM 3.1. *$k = Q(\sqrt{2}, \sqrt{p})$, p an odd prime, is Q-adequate if and only if p is not congruent to ± 1 mod 8.*

Proof. Each localization is the extension of the q-adic numbers Q_q which is obtained by adjoining roots of the polynomials $x^2 - 2$ and $x^2 - p$. These

polynomials give unramified extensions when $q \neq p$ or 2, and thus an extension of degree at most 2, for G_q must be a cyclic subgroup of $Z_2 \oplus Z_2$. To construct an element of order 4 in $H^2(k/Q)$ we must look to the primes 2 and p.

The polynomial $x^2 - p$ gives a quadratic totally-ramified extension of Q_p by Eisenstein's criterion ([*13*], 3–3–1). Hence we can have two local degrees of order 4 $\Leftrightarrow p$ is not a square in Q_2 and 2 is not a square in Q_p. But p is a square in $Q_2 \Leftrightarrow p \equiv 1$ (8); 2 is a square in $Q_p \Leftrightarrow (2/p) = 1 \Leftrightarrow p \equiv \pm 1$ (8) by (3.1). The local degree is 4 at 2 and at p unless $p \equiv \pm 1$ (8). The theorem follows by Proposition 2.5.

By the same reasoning, assuming p and q are odd primes:

THEOREM 3.2. *$k = Q(\sqrt{p}, \sqrt{q})$ is Q-adequate if and only if*

$$(p/q) = (q/p) = -1.$$

Proof. For $(p/q) = 1$ if and only if p is a square in Q_q, and the argument of Theorem 3.1 applies.

Theorem 3.2 shows that $Q(\sqrt{p}, \sqrt{q})$ is Q-deficient if $(p/q)(q/p) = -1$, and by (3.1) this happens whenever p and q are congruent to 3 modulo 4.

COROLLARY 3.3. *$Q(\sqrt{p}, \sqrt{q})$ is Q-deficient if $p \equiv 3$ (4) and $q \equiv 3$ (4).*

THEOREM 3.4. *Let $k = Q(\sqrt{-p}, \sqrt{q})$ for p and q rational primes. Then*

(1) *if $p = 2$, k is Q-adequate if and only if $q \equiv 5$ or 7 (8);*

(2) *if $q = 2$, k is Q-adequate if and only if $p \equiv 3$ or 5 (8);*

(3) *if p, q are odd, k is Q-adequate if and only if $(-p/q) = (q/p) = -1$.*

Proof. (1) q is a square at Q_2 if and only if $q \equiv 1$ (8); -2 is a square at Q_p if and only if $(-2/q) = 1$ if and only if $(-1/q)(2/q) = 1$ if and only if $q \equiv 1$ or 3 (8). Hence k is deficient if and only if $q \equiv 1$ or 3 (8).

(2) $-p$ is a square at Q_2 if and only if $p \equiv -1$ (8); 2 is a square at Q_p if and only if $p \equiv \pm 1$ (8). What remains is $p \equiv 3$ or 5 (8).

(3) is clear, for $-p$ is a square at Q_p if and only if $(-p/q) = -1$, etc.

4. CYCLOTOMIC FIELDS

$Q(m)$ will denote the splitting field of the polynomial $x^m - 1$ over Q. The aim of this section is to find for which m $Q(m)$ can be Q-adequate.

We review basic facts; details can be found in [*13*], Chapter 7.

(1) If p is an odd prime, s a positive integer, then $G(Q(p^s)/Q)$ is cyclic of order $p^{s-1}(p-1)$.

(2) If s is a positive integer,

$$G(Q(2^s)/Q) \cong \begin{cases} \text{trivial} & s = 1 \\ Z_2 & s = 2 \\ Z_2^{s-2} \oplus Z_2 & s \geqslant 3 \end{cases}$$

(3) If $(m, n) = 1$, then $G(Q(mn)/Q) \cong G(Q(m)/Q) \oplus G(Q(n)/Q)$.

(4) If $(2, m) = 1$, then $Q(m) = Q(2m)$.

Using (1) through (4) one can evaluate the Galois group of any cyclotomic field. To investigate which $Q(m)$ are Q-adequate we need the following key theorem.

THEOREM 4.1. *If G is Q-admissible, then every Sylow subgroup of G is metacyclic.*

DEFINITION. A finite group G is metacyclic if G has a normal subgroup H such that H is cyclic and G/H is cyclic (i.e., G is a cyclic extension of a cyclic group).

Proof of Theorem 4.1. Suppose $G = G(L/Q)$ and L is Q-adequate. Let P be a p-Sylow subgroup of G. By Proposition 2.6, $P \subset G_q$ for two different primes q. One of these primes, say t, is $\neq p$, and the residue class field of Q_t then has characteristic $\neq p$. In L_t/Q_t let M_t = the fixed field of P. Then $G(L_t/M_t) = P$ and hence L_t is a tamely-ramified extension of M_t. But all tamely-ramified Galois extensions of local fields have metacyclic Galois groups ([*13*], 3–5–3, 3–6–4). It follows that P is metacyclic.

We use Theorem 4.1 to settle the question of the adequacy of cyclotomic fields.

DEFINITION. Suppose p and q are distinct primes. Then $[p, q^r]$ = the order of p in the multiplicative group of units of the ring Z/q^rZ.

From the example after Proposition 2.6 and Proposition 2.1, $Q(m)$ is Q-deficient whenever $8 \mid m$. If $m = 4n$ with n odd, write $m = 4p_1^{l_1} \cdots p_r^{l_r}$. The Galois group of $Q(4n)/Q$ is then isomorphic to

$$Z_2 \oplus \sum_{i=1}^{r} (Z_{p_i - 1} \oplus Z_{p_i^{l_i - 1}})$$

which contains $Z_2 \oplus \cdots \oplus Z_2$ since $p_i - 1$ is even. Theorem 4.1 implies that $Q(4n)$ is deficient if $r > 1$.

We may asume $n = 4p^l$ for p an odd prime. Then $G(Q(m)/Q) \cong Z_2 \oplus Z_{p-1} \oplus Z_{p^{l-1}}$. $Q(m)$ is then unramified (hence cyclic) at Q_p unless $q = 2$ or p. By Remark 1 of Theorem 2.8 the only relevant Sylow subgroup is the one belonging to 2; all other Sylow subgroups are cyclic. This means that to decide the adequacy of $Q(4p^l)$ we need only settle the existence of an element of $H^2(Q(4p^l)/Q)$ of appropriate 2-power order. The situation hinges on the behavior of the local extensions at 2 and p.

The polynomial $x^{p^e} - 1$ gives a splitting field over Q_2 of degree f where $f = [2, p^e]$. The polynomial $x^4 - 1$ gives an extension of Q_2 of degree 2. Hence the local extension at 2 has degree $2f$.

These same polynomials give extensions of Q_p of degree $(p-1)p^{e-1}$ and g where $g = [p, 4]$. To have an element of sufficient 2-power order we must have $g = 2$, i.e., $Q(4p^e)$ is deficient if $p \equiv 1$ (4). When $p \equiv 3$ (4), then $g = 2$, and to have an element of maximum 2-power order we must have $2 \mid f$, i.e., $[2, p^e]$ is divisible by 2.

If $4 \nmid m$ we may as well assume that m is odd by (4) above. When $m = p_1^{e_1} \cdots p_r^{e_r}$ and $r > 2$, as before, the 2-Sylow subgroup is not metacyclic. We may assume $m = p^a q^b$ for distinct odd primes p and q. As before the field $Q(m)$ is unramified at Q_t unless $t = p$ or q. Thus we need only examine local behavior at p and q. The local extension at Q_p has degree $(p-1)p^{a-1}[q, q^b]$. Similarly, the extension at Q_p has degree $(q-1)q^{b-1}[q, p^a]$.

$G(Q(p^a q^b)/Q) \cong Z_{p-1} \oplus Z_{p^{a-1}} \oplus Z_{q-1} \oplus Z_{q^{b-1}}$. Let $p_1, \ldots, p_r$ be the odd primes which divide $p - 1$ *and* $q - 1$. Then the primes $2, p, q, p_i$ $(i = 1, \ldots, r)$ represent the only possible Sylow subgroups which are *not* cyclic. The maximal contributions for these primes must be made up at p and q, so we must have

(1) $[p, q^b]$ is divisible by the highest power of $2, p, p_i$ $(i = 1, \ldots, r)$ dividing $q - 1$ and by q^{b-1} if $q \mid p - 1$.

(2) $[q, p^a]$ is divisible by the highest power of $2, q, p_i$ $(i = 1, \ldots, r)$ dividing $p - 1$ and by p^{a-1} if $p \mid q - 1$. If (1) and (2) fail in any particular, then $Q(p^a q^b)$ is deficient; if they hold it is adequate over Q.

We gather all this together in

THEOREM 4.2. *The Q-adequacy of $k = Q(m)$ can be determined according to the following steps*:

(1) *If $8 \mid m$, k is Q-deficient.*

(2) *If $m = 4p_1^{e_1} \cdots p_e^{e_r}$ and $r > 1$, k is Q-deficient.*

(3) *If $m = 4p^e$, then k is Q-deficient when $p \equiv 1$ (4).*

(4) *If $m = 4p^e$ and $p \equiv 3$ (4), then k is Q-adequate if and only if $[2, p^e]$ is divisible by 2.*

(5) *If $m = 4$, k is Q-adequate.*

(6) *If $4 \nmid m$, assume m is odd; $m = p_1^{e_1} \cdots p_r^{e_r}$. Then k is Q-deficient when $r > 2$.*

(7) *If $m = p^a q^b$, let $p_1, \ldots, p_r$ be all odd primes which divide both $p - 1$ and $q - 1$. Then k is Q-adequate if and only if both* (i) *and* (ii) *below hold:*

(i) *$[p, q^b]$ is divisible by the highest power of p, q, p_i $(i = 1, \ldots, r)$ dividing $q - 1$ and by q^{b-1} if $q \mid p - 1$.*

(ii) *$[q, p^a]$ is divisible by the highest power of $q, 2, p_i$ $(i = 1, \ldots, r)$ dividing $p - 1$ and by p^{a-1} if $p \mid q - 1$.*

(8) *If $m = p^r$, then k is Q-adequate.*

5. Simultaneity

The classical theorem on division algebras over global fields says that every one such is cyclic. One may well ask whether cyclic maximal subfields are in any sense unique. We show in fact that this is far from the case. This being accomplished, we pose an opposite question of simultaneity: do a finite number of k-division rings of the same degree possess a cyclic maximal subfield in common? The concluding theorem of this section gives an affirmative answer to this question.

Definition. Suppose L, M are two Galois extensions of a global field k of the same degree. We will say L and M co-inhabit a k-division ring if there is a k-division ring D containing both L and M as maximal subfields.

Proposition 5.1. *Suppose L and M are two Galois extensions of a global field k of degree p^r, p a prime. Then L and M co-inhabit a k-division ring if and only if there are two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of k with $[L_{\mathfrak{p}_1} : k_{\mathfrak{p}_1}] = [L_{\mathfrak{p}_2} : k_{\mathfrak{p}_2}] = [M_{\mathfrak{p}_1} : k_{\mathfrak{p}_1}] = [M_{\mathfrak{p}_2} : k_{\mathfrak{p}_2}] = p^r$.*

Proof. Suppose D is a k-division ring containing L and M as maximal subfields. We look at $D \otimes_k k_{\mathfrak{p}} = D_{\mathfrak{p}}$ for $\mathfrak{p}$ running over the primes of k. The cohomology class X of $H^2(L/k)$ representing D has local component of order p^r at primes $q_1, \ldots, q_s$ where $s \geqslant 2$. The component of X in $H^2(L_{\mathfrak{p}_i}/k_{q_i})$ of course represents D_{q_i}. Then the cohomology class of $H^2(M/k)$ representing D must have local component of order p^r at $q_1, \ldots, q_s$, and this means $[L_{q_i} : k_{q_i}] = [M_{q_i} : k_{q_i}] = p^r$ for $i = 1, \ldots, s$.

Conversely, say L and M have local degree p^r at $\mathfrak{p}_1, \mathfrak{p}_2$. Select $a_i \in H^2(L_{\mathfrak{p}_i}/k_{\mathfrak{p}_i})$ and $b_i \in H^2(M_{\mathfrak{p}_i}/k_{\mathfrak{p}_i})$ $(i = 1, 2)$ so that a_1 and b_1 have invariant $1/p^r$ and a_2, b_2 have invariant $-1/p^r$. Then $a_1 + a_2$ represents a k-division ring

$D_1 \supset L$ as maximal subfield and $D_1 \otimes_k k_\mathfrak{p}$ is split except when $\mathfrak{p} = \mathfrak{p}_1, \mathfrak{p}_2$. Similarly $b_1 + b_2$ represents a k-division ring D_2 containing M as maximal subfield.

But $D_1 \otimes_k D_2^o$ (D_2^o = the opposite algebra) is split at all primes different from $\mathfrak{p}_1$ and $\mathfrak{p}_2$, and at these primes has invariant $1/p^r - 1/p^r = 0$. This means that $D_1 \otimes_k D_2^o$ is split at all primes of k and is thus a matrix algebra. Necessarily $D_1 = D_2$ (division rings in the same Brauer class are equal), so D_1 contains L and M as maximal subfield.

If k is a global field and L, M two cyclic extensions of k of degree p^r, then L and M co-inhabit a k-division ring if we can satisfy the conclusion of Proposition 5.1. This is in fact the case, and can be readily proved by density considerations. The proof below, which is entirely algebraic, was communicated to me by Whaples.

LEMMA 5.2. (Whaples). *Suppose k is an algebraic number field and L, M are two cyclic extensions of common degree p^r, p a prime. Then there are infinitely many primes of k which are inertial in both L and M.*

Proof. Let L_1 be the unique subfield of L of degree p over k, and similarly $M_1 \subset M$. If $\mathfrak{p}$ is unramified in L, the following are equivalent:

(a) $\mathfrak{p}$ is prime in L.

(b) $\mathfrak{p}$ does not split completely in L_1.

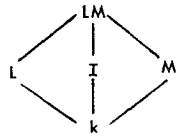
(c) $\mathfrak{p}$ is prime in L_1.

For if $\mathfrak{F}$ is any extension of $\mathfrak{p}$ to L and $D(\mathfrak{F})$ the decomposition field (depending only on $\mathfrak{p}$), all statements above are equivalent to the statement $D(\mathfrak{F}) = k$. Hence it is enough to satisfy the conclusion of Lemma 5.2 for L_1 and M_1, so we may suppose $r = 1$. By change of notation, we assume $[M : k] = [L : k] = p$.

If $M = L$ there is surely no difficulty; we assume $M \neq L$ and thus $M \cap L = k$. We define elements $\sigma, \tau \in G(LM/k)$ satisfying:

$$\sigma = \begin{cases} \text{generator of } G(LM/L) \\ \text{identity on } L \end{cases} \qquad \tau = \begin{cases} \text{generator of } G(LM/M) \\ \text{identity on } M \end{cases}$$

Let I = the fixed field of the group generated by $\sigma\tau$. We have the diagram:



It is clear that $LM = IM = IL$. Suppose $\mathfrak{p}'$ is a prime of I that does not extend a ramified prime of k to ML with $\mathfrak{p}'$ inertial in ML. Let $\mathfrak{p}$ be the restriction of $\mathfrak{p}'$ to k, and $\mathfrak{P}$ the unique extension of $\mathfrak{p}'$ to ML.

Since $\mathfrak{p}$ is unramified in ML, $G_1 = G(ML)_{\mathfrak{P}}/k\mathfrak{p})$ is a cyclic group. But $G(ML/k) \cong Z_p \oplus Z_p$ and $G_1 \subset G(ML/k)$. If G_1 is trivial we would conclude that $\mathfrak{p}$ factors into p^2 primes in ML, contradicting the fact that $\mathfrak{p}'$ is prime in ML. Hence $G_1 = Z_p$, and $\mathfrak{p}$ factors in I/k into p factors $\mathfrak{p}_1', \ldots, \mathfrak{p}_p'$ of degree 1 (all of which remain prime in ML/I).

Claim. $\mathfrak{p}$ remains prime in L/k and M/k. For if $\mathfrak{p}$ splits completely in L we would have $\mathfrak{p}$ split completely in I and L implying $\mathfrak{p}$ split completely in $IL = ML$, contradicting the choice of $\mathfrak{p}'$. By the equivalence of (b) and (c) $\mathfrak{p}$ is prime in L. By symmetry $\mathfrak{p}$ is prime in M. Since there were infinitely many choices for $\mathfrak{p}'$, there are infinitely many choices for $\mathfrak{p}$.

We observe with Whaples that the proof of Lemma 5.2 works in any "classical product formula field."

The fact that any two cyclic extensions of the same degree co-inhabit a single division ring is an easy consequence of Lemma 5.2.

THEOREM 5.3. *Suppose L, M are two extensions of an algebraic number field k, both cyclic of degree n. Then L and M co-inhabit a k-division ring.*

Proof. If $n = p^r$ for p a prime, we are finished by Proposition 5.1 and Lemma 5.2. Otherwise let $n = p_1^{e_1} \cdots p_r^{e_r}$. We may write L as a composite of fields $L_1, \ldots, L_r$ with $G(L_i/k)$ cyclic of degree $p_i^{e_i}$. Similarly, M is a composite of $M_1, \ldots, M_r$. Let D_i be a k-division ring in which L_i and M_i co-inhabit. Then $D = D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ is a k-division ring in which L and M co-inhabit.

Theorem 5.3 is in a sense best possible. The following examples show that the analogous statement is false if three cyclic extensions are prescribed, or if two noncyclic extensions are given in advance.

EXAMPLE 1. If $k_1 = Q(\sqrt{5})$, $k_2 = Q(\sqrt{41})$, and $k_3 = Q(\sqrt{41.5})$, then any Q-division ring containing k_1 and k_2 as maximal subfields cannot contain k_3.

Proof. Since $5 \equiv 1\ (4)$ and $41 \equiv 1\ (4)$ we have by (3.1)

$$\left(\frac{41}{5}\right) = \left(\frac{5}{41}\right).$$

But $(41/5) = (1/5) = 1$, so $(5/41) = 1$. Suppose $D \supset k_1$ and k_2 as maximal subfields. Then $D \otimes_Q Q_p = D_p$ is a division ring for say $p = q_1, \ldots, q_s$. No q_i can be equal to either 5 or 41 since $(5/41) = 1$ implies $Q_{41}(\sqrt{5}) = Q_{41}$

which implies D_{41} is split, and similarly for D_5. For every i, $(5/q_i) = (41/q_i) = -1$, for otherwise D would split at q_i. But then $(41.5/q_i) = (-1)(-1) = 1$ implies D cannot represent a division algebra containing k_3; any such would split at all of the q_i. (One must note that D splits at the infinite valuation since all fields involved are real.)

EXAMPLE 2. Let $L_1 = Q(\sqrt{2}, \sqrt{p_1})$ and $L_2 = Q(\sqrt{2}, \sqrt{p_2})$, $p_1 \neq p_2$, where L_1 and L_2 are Q-adequate via Theorem 3.1. Then no Q-division ring can contain L_1 and L_2 as maximal subfields.

Proof. L_1 can have local degree 4 only at 2 and p_1; L_2 can have local degree 4 only at 2 and p_2, and so Proposition 5.1 cannot be satisfied.

We can also have Theorem 5.3 the other way around with the division rings given and the maximal cyclic subfield "simultaneous."

THEOREM 5.4. *Suppose k is a global field and $D_1, \ldots, D_n$ are k-division rings of common degree n. Then the D_i, $(i = 1, \ldots, n)$ have a common maximal subfield which is cyclic; in fact, infinitely many nonisomorphic ones.*

Proof. Case 1. The degree n is a power of a prime, $n = p^r$. Suppose $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are all the primes of k at which some D_i does not split. By [12], Corollary 2 we can find a cyclic extension L of k of degree p^r which has local degree p^r at $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Since global splitting is equivalent to local splitting, L splits all the D_i. It follows that L is a maximal subfield of each D_i. As we are free to make specifications at primes other than $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, there are infinitely many choices for L.

Case 2. The degree n is arbitrary. Let $p_1, \ldots, p_r$ be the primes dividing n. Then for each i we can write

$$D_i = D_i^{(1)} \otimes_k D_i^{(2)} \otimes_k \cdots \otimes_k D_i^{(r)}, \tag{5.1}$$

where each $D_i^{(j)}$ of (5.1) has degree a power of p_j ([1], Theorem 18, p. 77). By Case 1 we can find a field L_j which is cyclic over k of degree a power of p_j and which is common maximal subfield of the $D_i^{(j)}$ for fixed j and $i = 1, \ldots, r$. Set $L = L_1 \otimes_k L_2 \otimes_k \cdots \otimes_k L_r$. L is the required field; it is cyclic, splits each D_i, and has the proper degree.

The question of common maximal subfields is an interesting one. Kaplansky has proved quite generally that any two quaternions over a field of characteristic not 2 have a common maximal subfield. For global fields this information is contained in Theorem 5.4, even for characteristic 2.

6. Abelian Extensions

In this section we finally settle which Abelian groups can be Q-admissible. There are no surprises; they are exactly the ones predicted by Theorem 4.1.

We conclude this section with a proof of a kind of fundamental existence theorem: for any finite Abelian group A there is an algebraic number field k with A k-admissible. What's more, all Abelian groups of a given order can even be accounted for "simultaneously" within the same division ring. For non-Abelian groups the fundamental theorem still holds, although the proof is entirely different. However, the simultaneity condition is perhaps not true in the non-Abelian case. For that reason we include a separate discussion of the Abelian case.

Theorem 6.1. *An Abelian group A is Q-admissible if and only if every Sylow subgroup of A is metacyclic (A is a direct sum of two cyclic groups).*

Proof. The sufficiency condition is clear by Theorem 4.1.

Necessity: Suppose first A is isomorphic to $Z_{p^r} \oplus Z_{p^s}$, p a prime. Let m = maximum of r and s. If we choose rational primes q_1 and q_2 different from 2 and satisfying $q_i \equiv 1(p^m)$, $i = 1, 2$, then the equation $x^{q_i} = 1$ gives a totally ramified extension of Q_{q_i} of degree $q_i - 1$. Since p^m divides $q_i - 1$, we conclude that Q_{q_i} has a totally-ramified extension of degree p^m. Of course, local fields have unramified extensions of all degrees, and totally-ramified extensions are disjoint from unramified ones.

Suppose L_i is an extension of Q_{q_i} which is cyclic totally ramified of degree p^r and M_i an extension of Q_{q_i} which is unramified, and so cyclic, of degree p^s.

By Wang's theorem ([3], Theorem 5, p. 105) there is a cyclic extension L of Q of degree p^r and a cyclic extension M of Q of degree p^s with $L_{q_i} = L_i$ and $M_{q_i} = M_i$, $i = 1, 2$. Clearly LM has Galois group $Z_{p^r} \oplus Z_{p^s}$ over Q since this is also the Galois group at q_1 and q_2. As the local extensions of LM at the q_i have degree p^{r+s}, LM is Q-adequate by Proposition 2.5.

To complete the proof of Theorem 6.1 suppose $p_1, \ldots, p_r$ are the primes dividing $|A|$, and D_i ($i = 1, \ldots, r$) are Q-division rings showing the p_i-Sylow subgroup of A to be Q-admissible. Then $D_1 \otimes_k \cdots \otimes_k D_r$ is a Q-division ring showing A to be admissible over Q.

It should be noted here that Theorem 6.1 gives rise to a host of "distinguishing" polynomials. If A is a finite Abelian group which is not Q-admissible, there is by class field theory a Galois extension L of Q with $A = G(L/Q)$. We may write $L = Q(\alpha)$ for α a root of a monic irreducible polynomial $f(x)$ over Q. By Proposition 2.1, $f(x)$ is distinguishing; any division ring with Q as center which contains a root of $f(x)$ is infinite dimensional.

Another measure of the failure of Theorem 4.1 for arbitrary number fields is the following theorem, which says that any Abelian group is admissible if the base field is not specified in advance.

THEOREM 6.2. *Let A be any finite Abelian group. Then for some algebraic number field k, A is k-admissible.*

Proof. Assume first that A is a p-group,

$$A \cong Z_{p^{e_1}} \oplus \cdots \oplus Z_{p^{e_r}} .$$

Let k be any algebraic number field satisfying:

(1) p splits in k,

(2) $k \supset$ the p^sth roots of unity for $s = \max(e_i)$, $i = 1,..., r$.

(3) The localizations of k at two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ extending p are large enough so that A appears as a Galois group over $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$.

To justify (3) we observe with Serre ([8], Proposition 10, p. 220 and (iii) of Corollary 2, p. 225) that if K is a local field, $[K : Q_p] = n$, then the subgroup U^1 of the units U_K is a product of a finite cyclic group by an Abelian pro-p group free on n letters. Since U^1 is of finite index in U_K and

$$G_{ab}(K) \cong \hat{Z}XU_K$$

where $G_{ab}(K)$ is the group of the maximal Abelian extension of K and $\hat{Z}$ is topologically free on one generator, we conclude A is a homomorphic image of $G_{ab}(K)$ if $n \geqslant r$. Hence (3) is satisfied if the local degrees at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are larger than r. Satisfying (1) and (2) is child's play.

We may assume $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$ admit normal extensions L_1 and L_2 such that: $G(L_i/k_{\mathfrak{p}_i}) = A$. Now write L as a composite:

$$L_i = L_{i1} \cdots L_{ir}$$

where $G(L_{ij}/k_{\mathfrak{p}_i}) = Z_{p^{e_j}}$. By condition (2) and Kummer Theory the extensions L_{ij} is the splitting field of a polynomial $x^{p^{e_j}} - a_{ij}$ for a_{ij} an integer of $k_{\mathfrak{p}_i}$. Select b_j an integer of k so that b_j is close enough to a_{ij} in the topology determined by $\mathfrak{p}_i$ to insure that the polynomial $x^{p^{e_j}} - b_j$ determines the same splitting field over $k_{\mathfrak{p}_i}$ as $x^{p^{e_j}} - a_{ij}$ ([13], Exercise 3-2). By choice of the b_j,

$$k_{\mathfrak{p}_i}[(b_j)^{1/p^{e_j}}] = L_{ij}$$

for $i = 1, 2$ and $j = 1,..., r$. Let

$$M_j = k[(b_j)^{1/p^{e_j}}].$$

By Kummer Theory M_j/k is cyclic and $G(M_j/k) = Z_{p^{e_j}}$, since M_j has local degree p^{e_j} at $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

Write $M = M_1M_2 \cdots M_r$. Clearly $G(M/k) = A$, for this happens at $\mathfrak{p}_1$ and $\mathfrak{p}_2$. By Proposition 2.5, M is k-adequate, and so A is k-admissible.

To complete the proof of Theorem 6.2, let A be any finite Abelian group and $|A| = p_1^{e_1} \cdots p_r^{e_r}$. We choose an algebraic number field k satisfying

(1′) k splits at $p_1, \ldots, p_r$,

(2′) $k \supset$ the $|A|$-th roots of 1,

(3′) for each $i = 1, \ldots, r$ there are primes spots $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of k extending p_i such that $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$ admit the p_i-Sylow subgroup of A as the Galois group of a normal extension.

According to the argument which preceded, every p_i-Sylow subgroup of A is k-admissible; suppose a k-division ring D_i realizes this admissibility. Then clearly $D = D_1 \otimes_k \cdots \otimes_k D_r$ shows A to be k-admissible.

There is a lot more to win from Theorem 6.2 by squeezing harder. Suppose, for instance, that $n = p^s$ and k is an algebraic number field satisfying

(1*) k splits at p,

(2*) $k \supset$ the nth roots of 1,

(3*) k has localizations $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$ extending Q_p and satisfying: Any Abelian group of order n is a Galois group over $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$.

That we can find such a k is obvious from the proof of Theorem 6.2. Then if A is a given Abelian group of order n, we select (as in the proof of Theorem 6.2) a k-division ring D which shows A to be k-admissible and which splits everywhere but at $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$. Suppose B is any other Abelian group of order n. Just as in the proof of Theorem 6.2 we can find a normal extension M of k so that $G(M/k) = B$ and M has local degree n at $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$. It follows that M splits D, ergo $M \subset D$. Collecting the pieces, we have proved

PROPOSITION 6.3. *If $n = p^s$ as above, then there is an algebraic number field k and a division ring D central on k satisfying: Any Abelian group of order n is the Galois group of a normal maximal subfield of D.*

The following theorem shows generally that not only are Abelian groups of a given order admissible, but all Abelian groups of the same order are simultaneously admissible.

THEOREM 6.4. *Suppose an integer n is given. Then there is an algebraic number field k and a k-division ring D satisfying: Any Abelian group of order n is the Galois group of a normal maximal subfield of D.*

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$. We select k so that Proposition 6.3 holds over k for each $p_i^{e_i}$. Then there are k-division rings D_i $(i = 1,..., r)$ so that D_i shows every Abelian group of order $p_i^{e_i}$ to be k-admissible. Clearly then $D = D_1 \otimes_k \cdots \otimes_k D_r$ shows every Abelian group of order n to be k-admissible.

7. The Rationals

Among the questions left unanswered by Theorems 6.1 and 6.4 are

(1) Which groups are Q-admissible?

(2) Given a finite group G, is there an algebraic number field k so that G is k-admissible?

We shall answer (2) in the affirmative presently. Question (1) has been answered in detail for Abelian groups; in this section we answer it at least for symmetric groups.

In all that follows S_n will denote the symmetric group on n letters. Note that S_6 is not Q-admissible, for its 2-Sylow subgroup is the product of a dihedral group of order 8 (written D_8) by a cyclic group of order 2. This group is not metacyclic; by Theorem 4.1, S_6 is not Q-admissible. It follows of course that S_n is not Q-admissible for $n \geqslant 6$, for the 2-Sylow subgroup of such a group contains a 2-Sylow subgroup of S_6, and the property of being metacyclic is preserved in taking subgroups.

Our list of Q-admissible groups is not very large. Besides the Abelian ones we can point only to the totally admissible ones of Theorem 2.8. Based on such a list one may well conjecture that any Q-admissible group must be solvable; we will presently show this to be false. However, the converse of Theorem 4.1 may very well be true, but the difficulties in making a proof are overwhelming.

The projective linear groups $PSL(2, p)$, p prime, all have metacyclic Sylow subgroups. However, it is not known whether such groups appear as Galois groups over the rationals, and Q-admissibility asks for far more even than that.

Theorem 7.1. *S_n is Q-admissible $\Leftrightarrow n \leqq 5$.*

Proof. We have dealt with $n \geqslant 6$ above. Since S_2 and S_3 are totally admissible, they are Q-admissible (Theorem 2.8). Hence we are left only with the cases $n = 4$ or 5. We will do the case $n = 5$ in detail; the case $n = 4$ will follow from the same proof with the obvious modifications.

The 2-Sylow subgroup of S_5 is the dihedral group of order 8, which we will write D_8. Our problem is to show it can be a Galois group over enough

local fields. This is accomplished by quoting the following theorem of Albert [2], Theorem 9.

LEMMA 7.2. (Albert). *Q_p has a tamely-ramified Galois extension of degree ef if and only if $(e, p) = 1$ and G is generated by two elements S and T satisfying*

(1) $S^f = T^i$;
(2) $T^e = 1$;
(3) $TS = ST^p$;
(4) $e \mid p^f - 1$, $e \mid i(p-1)$;
(5) $0 \leqslant i < p^f - 1$;

In Lemma 7.2 we let $f = 2$, $e = 4$, and $i = 4$. p is to be determined. Then $S^2 = T^4 = 1$ and $ST^p = TS$ or $STS = T^p$. When $p \equiv 3\ (4)$ these equations become:

$$S^2 = T^4 = 1, \qquad STS = T^3 = T^{-1}. \tag{7.1}$$

It is well known that (7.1) is nothing more than the describing relations for D_8. We have proved

COROLLARY 7.3. *Q_p has a Galois extension with group D_8 whenever $p \equiv 3\ (4)$.*

Suppose L is an extension of Q_p with Galois group D_8. We consider the fixed field M of the subgroup generated by S of (7.1). This group is not normal, for $TST^{-1} = TST^3 = ST^3 \cdot T^3 = ST^2 \notin \{S\}$. Hence M is not a normal extension of Q_p. We write $M = Q_p(\alpha)$ where α is integral. Suppose $f(x)$ is the irreducible nomic polynomial for α over Q_p. The coefficients of $f(x)$ are p-adic integers and L is the splitting field for $f(x)$ over Q_p (M is not normal). The upshot: We have proved L is the splitting field over Q_p of a polynomial with integral coefficients of degree 4.

To finish the proof of Theorem 7.1, pick primes p_1 and p_2 so that D_8 appears over Q_{p_i}, $i = 1, 2$. Select a polynomial $f(x) \in Z[x]$ so that:

(1) $f(x)$ is "close to" $f_i(x)(x - a_i)$ in the p_i-adic topology, where a_i is any p_i-adic integer, and $f_i(x)$ is a polynomial of degree 4 whose split field over Q_{p_i}, say L_i, has Galois group D_8. How close "close to" is will be determined.

(2) $f(x)$ is close to $f_3(x)$ in the q-adic topology for $q \neq p_1, p_2$, where $f_3(x)$ is irreducible of degree 5 over Q_q (monic with integral coefficients).

"Close to" in (1) and (2) means close enough so that $f(x)$ has a splitting field containing L_i at Q_{p_i} and $f(x)$ stays irreducible at the prime q. (See [13],

3-2-5, Exercise 3-2 and 4-1-8). Let L be the splitting field for $f(x)$ over Q. Then $G(L_{\mathfrak{p}_i}/Q_{\mathfrak{p}_i}) = D_8$ by condition (1).

Claim. $G = G(L/Q) = S_5$.

Proof. Certainly $G \subset S_5$ since $f(x)$ is irreducible of degree 5 over Q. But the remarks above show D_8 is a subgroup of G. It it well known that a subgroup of S_5 which contains a transposition and an element of order 5 is S_5. Ergo $G = S_5$.

Certainly $H^2(L/Q)$ has an element of order 8 by applying Proposition 2.5 to the primes p_1 and p_2 of Q. That it has an element of order 15 is clear; the 5-Sylow and 3-Sylow subgroups of S_5 are cyclic. Ergo $H^2(S_5, L^*)$ has an element of order 120, which shows that L is Q-adequate and S_5 is Q-admissible.

It is still undetermined whether the alternating groups A_4, A_5, A_6, and A_7 are Q-admissible. It would be desirable to deduce Q-admissibility of A_4 and A_5 from the admissibility of S_4 and S_5. Unfortunately, our procedure of passing to subgroups is accomplished only at the price of raising the base field. Nevertheless, we conjecture that raising the base field is not really necessary.

Conjecture. If G is k-admissible and H a subgroup of G, then H is k-admissible.

The other alternating groups are no problem.

THEOREM 7.4. *A_n is not Q-admissible for $n \geqslant 8$.*

Proof. The 2-Sylow subgroup of any such group contains $Z_2 \oplus Z_2 \oplus Z_2$, and is not metacyclic.

8. LOCAL FIELDS AND p-GROUPS

We review first some basic facts about p-groups. All this information is quite standard and can be found for instance in [5].

Suppose G is a finite p-group. Let $F(G)$ be the subgroup of G generated by all commutators and pth powers of elements in G. $F(G)$, the Frattini subgroup of G, is a normal subgroup and the quotient $G/F(G)$ is an elementary p-group. Suppose $d(G)$ = the dimension of $G/F(G)$ as a vector space over Z_p. Burnside's basis theorem says that any minimal set of generators for G contains $d(G)$ generators.

Of special concern for us will be the Sylow subgroups of symmetric groups. Accordingly, let p be any prime. We wish to determine the p-Sylow subgroup of S_n.

If we write n in the scale of p:

$$n = a_0 p^u + a_1 p^{u-1} + \cdots + a_{u-1} p + a_u, \qquad 0 \leqslant a_i < p \qquad (8.1)$$

then a p-Sylow subgroup P of S_n has order p^t where

$$t = a_0(p^{u-1} + p^{u-2} + \cdots + p + 1) + a_1(p^{u-2} + p^{u-3} + \cdots) + \cdots + a_1 .$$

Further, if we divide the n letters into a_0 blocks of p^u letters, a_1 blocks of p^{u-1} letters,..., and a_{u-1} blocks of p letters, then P can be written as a direct product:

$$P \cong \underbrace{P_u \times P_u \cdots \times P_u}_{a_0 \text{ copies}} \times \underbrace{P_{u-1} \times \cdots \times P_{u-1}}_{a_1 \text{ copies}} \times \cdots \times \underbrace{P_1 \times \cdots \times P_1}_{a_{u-1} \text{ copies}} \tag{8.2}$$

where P_u denotes a p-Sylow subgroup of the symmetric group on p^u letters.

To determine the p-Sylow subgroups of S_n we thus need only determine the p-Sylow subgroup of S_{p^u}. This is described quite explicitly by iterated wreath products in [5], but this full description is not necessary. As much as we will need is contained in the proposition below; the proof was suggested to me by Jon Alperin.

PROPOSITION 8.1. *With notation as above, assume $u > 1$. Then P_u contains a subgroup H satisfying:*

(1) $[P_u : H] = p^u$.

(2) *The only subgroup of H normal in P_u is the identity.*

Proof. Let the letters permuted be $a_1, \ldots, a_{p^u}$ and H the subgroup of P_u fixing the first letter a_1. We devise a map from the left cosets of H in P_u into the letters $a_1, \ldots, a_{p^u}$ via

$$gH \rightsquigarrow g(a_1). \tag{8.3}$$

It is trivial to verify that the map (8.3) is well defined and 1–1. It is onto if and only if P_u is transitive on the p^u letters. But the p^u cycle $(a_1, \ldots, a_{p^u})$ is in some p-Sylow subgroup of S_{p^u}, so a conjugate of it is in P_u. Since conjugacy preserves cycle structure, P_u contains a p^u cycle, say $\alpha = (a_1, a_{i_2}, \ldots, a_{i_{p^u}})$. Then α^s maps $a_1 \to a_{i_s}$, which shows that P_u is transitive. The map (8.3) is then 1–1 and onto, proving $[P_u : H] = p^u$.

To verify (2), suppose a subgroup K of H is normal in P_u. Then

$$gKg^{-1} = K \qquad \text{for} \quad g \in P_u .$$

It is clear that gKg^{-1} fixes $g(a_1)$, so K fixes $g(a_1)$. By transitivity of P_u any letter is a $g(a_1)$ for appropriate $g \in P_u$. Therefore K fixes every letter, from whence $K = \{1\}$.

The corollary and proposition to follows are the whole point of our discussion of Sylow subgroups of symmetric groups. Recall that in the proof of Theorem 7.1 we needed to conclude that a field extension with a given

Galois group is the splitting field of a polynomial of reasonably small degree. Sylow subgroups of symmetric groups can be quite large, but the next two results show the resulting polynomials are still manageable. Of course, there is still the problem of whether these groups can be Galois groups in the first place; we get to this matter at the end of this section.

COROLLARY 8.2. *Suppose L and k are any two fields with L a Galois extension of k and $G(L/k) = P_u$. Then L is the splitting field over k of a polynomial of degree p^u.*

Proof. In L we take the fixed field K of H specified by Proposition 8.1. One should note that the corollary is trivial if $u = 1$. Then $[K : k] = p^u$. We may write $K = k(\alpha)$, where the monic irreducible polynomial $f(x)$ of α over k has degree p^u. Surely L contains a splitting field of $f(x)$. Suppose k_0 is the splitting field for $f(x)$ in L. Then $L \supset k_0 \supset K \supset k$. If $H_0 = G(L/k_0)$, then H_0 is a normal subgroup of $P_u$contained in H. By Proposition 8.1, $H_0 = \{1\}$ and so $k_0 = L$.

THEOREM 8.3. *Let P be a p-Sylow subgroup of S_n, and L a Galois extension of a field k with $G(L/k) = P$. Then L is the splitting field over k of a monic polynomial of degree n.*

Proof. Recall that if we write n in the scale of p as in (8.1), we obtain a decomposition for P as in (8.2). Thus L is a composite of fields

$$L = L_{u,1} \cdots L_{u,a_0} L_{u-1,1} \cdots L_{1,1} \cdots L_{1,a_{u-1}}$$

where each $L_{i,j}$ is normal over k with $G(L_{i,j}/k) = P_i$.

By the last corollary each $L_{i,j}$ is the splitting field of a monic polynomial of degree p^i, say f_{ij}. Let

$$f = \prod_{i,j} f_{ij}.$$

Then L is the splitting field of f over k, and the degree of f is $n_0 = a_0 p^u + a_1 p^{u-1} + \cdots + a_{u-1} p \leqslant n$. By tacking on linear factors if necessary we can make the degree of $f = n$.

Remark. If L and k are local fields, we can insist that the polynomials of Theorem 8.3 have coefficients which are k-integers.

The logical question posed by the last remark is this: Can P appear as a Galois group of a pair of local fields? The answer is yes, due to highly nontrivial theorems of Demuskin and Shafarevic ([*4*], Theorem 1, and [*11*], Theorem 1). A discussion of Demuskin's theorem also occurs in [*9*]. We state these results without proof.

THEOREM 8.4. (Shafarevic). *Suppose K is a local field of degree n over the rational p-adic field. If K contains no pth root of unity, then the Galois group of the maximal p-extension of K, written $G_p(K)$, is free* pro-p *on $n+1$ generators.*

THEOREM 8.5 (Demuskin). *Suppose K is a local field of degree n over the rational p-*adic *field. Let p^s be the highest power of p such that K contains the p^sth roots of unity. Assume finally, $p^s \neq 2$. Then $G_p(K)$ can be generated by $n+2$ elements $\sigma_1, \ldots, \sigma_{n+2}$ satisfying the unique relation*

$$\sigma_1^{p^s}[\sigma_1, \sigma_2][\sigma_3, \sigma_4] \cdots [\sigma_{n+1}, \sigma_{n+2}], \qquad [a, b] = aba^{-1}b^{-1}. \tag{8.4}$$

Setting all odd σ_i in (8.4) equal to one, it follows that $G_p(K)$ has a homomorphic image which is free pro-p on $(n+2)/2$ generators. We conclude that for any local field K satisfying the conditions of either Theorem 8.4 or Theorem 8.5, and any finite p-group G, K has a normal extension with Galois group G whenever $d(G) \leqslant (n+2)/2$.

9. THE MAIN THEOREM

We are now in a position to prove the basic existence theorem; for any finite group G there is an algebraic number field over which G is admissible. The proof is simply an exercise in collecting the pieces. After reducing to the case $G = S_n$, we show that the Sylow subgroups of G appear as Galois groups over suitable local fields; these Galois extensions are splitting fields of polynomials which have relatively small degree. With this in mind the proof is nothing more than a mimicking of Theorem 7.1.

THEOREM 9.1. *For any finite group G there is an algebraic number field k with G k-admissible.*

Proof. Because of Proposition 2.9, we may assume $G = S_n$. Construct a field k satisfying:

(1) Every rational prime dividing $n!$ splits in k.

(2) k contains the 4th roots of unity.

(3) For every p dividing $n!$ there are prime spots $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of k such that the p-Sylow subgroup of S_n appears as a Galois group over $k_{\mathfrak{p}_1}$ and $k_{\mathfrak{p}_2}$.

Theorems 8.4 and 8.5 show that (3) is satisfied if the degrees of the $k_{\mathfrak{p}_i}$ over the p-adic field Q_p are large enough.

According to (3) we can select $L_{\mathfrak{p}_i}$ normal over $k_{\mathfrak{p}_i}$ so that $G(L_{\mathfrak{p}_i}/k_{\mathfrak{p}_i}) = P$, the relevant p-Sylow subgroup of S_n. By Theorem 8.3 each $L_{\mathfrak{p}_i}$ is the

splitting field over $k_{\mathfrak{p}_i}$ of a monic polynomial with integer coefficients and degree n, say $f_{\mathfrak{p}_i}$.

Let $f(x)$ be a polynomial monic with k-integer coefficients and of degree n satisfying the following: $f(x)$ is suitably close to $f_{\mathfrak{p}_i}$ in the $\mathfrak{p}_i$-topology to ensure that the splitting field of $f(x)$ over $k_{\mathfrak{p}_i}$ contains $L_{\mathfrak{p}_i}$. This is to hold for all the $\mathfrak{p}_i$ in (3) extending those rational primes which divide $n!$.

We can construct such a polynomial $f(x)$ by the strong approximation theorem ([*13*], 4-1-4) and the fact that "close" polynomials give comparable splitting fields.

Let M be the splitting field of $f(x)$ over k. We claim that $G(M/k) = S_n$. For certainly $G \subset S_n$ as $f(x)$ is a polynomial of degree n. But M was constructed to guarantee that $M_{\mathfrak{p}_i} \supset L_{\mathfrak{p}_i}$ for the $\mathfrak{p}_i$ of (3). It follows that $G(M_{\mathfrak{p}_i}/k_{\mathfrak{p}_i})$ is a subgroup of S_n containing a p-Sylow subgroup of S_n. Clearly then $G = S_n$.

The construction of $M_{\mathfrak{p}_i}/k_{\mathfrak{p}_i}$ and Proposition 2.5 then imply that $H^2(S_n, M^*)$ has an element of order $n!$, and so S_n is k-admissible.

Note that the fields of Theorem 9.1 are by no means unique. In fact, the fields k we obtain in the proof of the admissibility of S_n can be replaced by any finite extension of k.

10. Boundedness Conditions

Although all groups are admissible over suitable number fields, there are severe limitations on which groups can be admissible over a given number field. Theorem 6.1 is already an indication of this. In this section we show that the p-groups and symmetric groups which are k-admissible for a given algebraic number field k are "bounded".

Theorem 10.1. *Let k be an algebraic number field, $[k : Q] = n$, and G a p-group for a given prime p. If G is k-admissible, then $d(G) \leqq (n/2) + 2$.*

Proof. If G is metacyclic, the inequality is automatic. Otherwise the rational prime p splits in k, and the degree of each extension of p is at most $n/2$. For G to be k-admissible there must be a Galois extension L of k with $G(L_{\mathfrak{p}_i}/k_{\mathfrak{p}_i}) = G$ for two primes $\mathfrak{p}_i$ extending p, $i = 1, 2$. But by [7], Theorem 4, II-30 the Galois group of any p-extension of $k_{\mathfrak{p}_i}$ can be generated by $(n/2) + 2$ elements.

Note that Theorem 10.1 is only a partial generalization of Theorem 4.1 to k. The difficulty is that the proof of Theorem 4.1 required only one localization of Q for which the residue class field has characteristic p. This of course may be false in k. The next theorem is a generalization under special assumptions.

THEOREM 10.2. *Let k be an algebraic number field in which the prime p has a unique extension. Suppose G is k-admissible. Then the p-Sylow subgroup of G is metacyclic.*

Proof. Exactly as in Theorem 4.1.

Any finite group can be made admissible over a suitable number field by Theorem 9.1. In fact this is the most one can prove; the global fields of nonzero characteristic are unsuitable for this purpose.

THEOREM 10.3. *Let k be a global field of characteristic $p \neq 0$. If G is k-admissible, then every q-Sylow subgroup of G is metacyclic for $q \neq p$.*

Proof. Suppose P is a q-Sylow subgroup of G, $q \neq p$. By Proposition 2.5 there are Galois extensions of localizations $k_{\mathfrak{p}_1}, k_{\mathfrak{p}_2}$ with Galois group containing P. But all the $k_{\mathfrak{p}}$ have characteristic p for primes $\mathfrak{p}$ of k. By the Galois correspondence, P is a Galois group of a pair of local fields of characteristic p. As in the proof of Theorem 4.1 we conclude that any such extension is tamely ramified and therefore P is metacyclic.

As a consequence of Theorem 10.2 there are groups which are "absolutely inadmissible" in the context of function fields.

COROLLARY 10.4. *S_9 is not k-admissible for any global field k of nonzero characteristic.*

Proof. The 2-Sylow and 3-Sylow subgroups are not metacyclic.

Of course, there are no "absolutely inadmissible" groups in the context of algebraic number fields. However, the symmetric groups which are admissible over a given number field k are bounded in a manner analogous to Theorem 10.1.

To prove this we first outline the manner in which it can be false. Suppose k is an algebraic number field with the property that S_n is k-admissible for every n. In all that follows we discuss only localizations $k_{\mathfrak{p}}$ for $\mathfrak{p}$ extending 2. Since every S_n is k-admissible, there must be a Galois extension of some $k_{\mathfrak{p}}$ with Galois group G where G satisfies

(1) $G \subset S_n$; and

(2) $G \supset$ a 2-Sylow subgroup of S_n.

The following proposition effectively bounds the Galois groups satisfying (1) and (2). I would like to thank Walter Feit for supplying most of the group theory in the proof below.

To fix notation, we will write $[G : H]$ for the index of a subgroup H in a finite group G, and $\{x\}$ for the cyclic group generated by an element x of G.

PROPOSITION 10.5 (Feit). *Suppose G is a Galois group over a local field k satisfying*

(1) $G \subset S_n$;

(2) $G \supset$ *a 2-Sylow subgroup of* S_n. *Then* $|G| = 2^a 3^b$ *where* $b = 0$ *or* 1.

Proof. We may as well assume that the residue class field of k has characteristic 2; otherwise the 2-Sylow subgroup of G is metacyclic and the proposition is true by inspection. By local ramification theory G has normal subgroups τ and V so that

(a) $G \supset \tau \supset V$,

(b) G/τ is cyclic,

(c) τ/V is cyclic of order prime to 2,

(d) V is a 2-group.

Here τ corresponds (in the Galois correspondence) to the maximal unramified subfield, and V to the maximal tamely-ramified subfield.

Let S be 2-Sylow subgroup of S_n in G. Then $[S, S] \subset \tau$ by (b), and $S \cap \tau = V$ by (c). It follows that $[S, S] \subset V$, and so $[S : V] \leqq 2$ as $[S, S]$ is the Frattini subgroup of S. Let U be a p-Sylow subgroup of G for some prime $p \neq 2$. We claim that U is cyclic. To prove that U is cyclic, it is enough to prove $p \nmid |G/\tau|$.

Suppose $p \mid |G/\tau|$. Then G has a normal subgroup, say N, of index p, and $S \subset N$. Let $g \in G, g \notin N$. Then for some $n \in N$, $S^g = S^n \Rightarrow gn^{-1}$ normalizes S. As S is self-normalizing in S_n, we conclude $gn^{-1} \in S$ and so $g \in N$, a contradiction. It follows that U is cyclic.

Suppose $U = \{x\}$ is a p-Sylow subgroup of G, $p \neq 2$. We are finished if we can show $x^3 = 1$. The proof will be by induction on n. We think of G as permutations on letters $1,\ldots, n$.

Case I. The orbits of $V =$ the orbits of S.

Let $A_1, \ldots, A_r$ be the orbits of S with A_r smallest. Since x normalizes V, the A_i are permuted by x, so necessarily $x : A_i \to A_i$ as all A_i have different orders. But then $x : A_r \to A_r$, and x has a fixed point, say 1, in A_r.

Let $F_1 = \{\sigma \in G \mid \sigma(1) = 1\}$.

F_1, considered as permutations on the letters $2,\ldots, n$, contains a 2-Sylow subgroup of S_{n-1}; in fact $S \cap F_1$ is a 2-Sylow subgroup of S_{n-1} in F_1 by the argument of Proposition 8.1. Since $x \in F_1$, $x^3 = 1$.

Case II. The orbits of $V \neq$ the orbits of S.

If $x : A_r \to A_r$, we are finished as before. As x still preserves the orbits of V and $[S : V] \leqq 2$, the only alternative is that $A_{r-1} = A_{r-1}^{(1)} \cup A_{r-1}^{(2)}$ with

$A_{r-1}^{(i)}$ $(i = 1, 2)$ orbits under V, $|A_{r-1}^{(i)}| = |A_r|$, and x permutes $A_{r-1}^{(1)}$, $A_{(r-1)}^{(2)}$, A_r. Further, V projects onto a full 2-Sylow subgroup of the letters in A_i, $i \neq r-1$, for otherwise $[S : V]$ would be >2. Since x normalizes V, it normalizes the action of S on the A_i, and so $x = 1$ on A_i, $i \neq r-1, r$.

But $x^3 : A_r \to A_r$, and V projects onto a full 2-Sylow subgroup of the letters in A_r, so $x^3 = 1$ on A_r. Suppose $m \in A_{r-1}^{(i)}$. Then $x(m) \in A_r$ or $x^2(m) \in A_r$. In any case

$$x^3(x(m)) = x(m) \qquad \text{or} \qquad x^3(x^2(m)) = x^2(m),$$

and cancellation gives $x^3(m) = m$. Thus $x^3 = 1$ on every A_i, so $x^3 = 1$.

COROLLARY 10.6. *Suppose k is an algebraic number field with $[k : Q] = m$. Let $d_2(S_n)$ be the minimal number of generators of a 2-Sylow subgroup of S_n. Then if S_n is k-admissible, $d_2(S_n) \leqq 3m + 2$. In particular, only finitely many S_n are k-admissible.*

Proof. By Proposition 2.6, some localization $k_\mathfrak{p}$ of k has a Galois extenion L with Galois group G satisfying: $G \subset S_n$ and $G \supset$ a 2-Sylow subgroup of S_n. Let M correspond to the 2-Sylow subgroup of G. Then $[M : Q_2] \leqq 3m$, and $P = G(L/M)$ is a 2-Sylow subgroup of S_n by Proposition 10.5. It follows that $d(P) = d_2(S_n) \leqq 3m + 2$.

Although Corollary 10.6 shows that only finitely many S_n are k-admissible, it gives no hint as to the manner in which the S_n appear. It is perhaps possible that S_{n+1} is k-admissible while S_n is not.

We conclude with the long-delayed counterexample to the converse of Corollary 2.4.

Let $L = Q(\alpha)$, where α is a root of a monic irreducible polynomial of degree 7 over Q. If $\tilde{L}$ is the normal closure of L, we assume that $G(\tilde{L}/Q) = S_7$. By Theorem 7.1, $\tilde{L}$ is not Q-adequate.

Claim. L is Q-adequate.

There is an exact sequence

$$0 \to B(L/Q) \to B(\tilde{L}/Q) \xrightarrow{j} B(\tilde{L}/L).$$

Since the 7-Sylow subgroup of S_7 is cyclic, $B(\tilde{L}/Q)$ has an element of order 7 by Remark 1 of Theorem 2.8. Suppose x in $B(\tilde{L}/Q)$ has order 7.

The dimension of $\tilde{L}$ over L is prime to 7, so $j(x) = 0$. Ergo x is in $B(L/Q)$. Since $B(L/Q)$ has an element of order 7, we conclude that L is Q-adequate.

Of course, the proof above applies for 7 replaced by any prime larger than 5. For those with a more literal turn of mind the proof could be restated as follows: If D is the underlying division ring of any element of $B(\tilde{L}/Q)$ of order 7, then D contains every subfield of $\tilde{L}$ which is of degree 7 over Q as a maximal subfield.

ACKNOWLEDGMENT

Many thanks are due to Professor I. N. Herstein for his advice in the preparation of this paper.

REFERENCES

1. ALBERT, A. A. "Structure of Algebras." American Mathematical Society, New York, 1939.
2. ALBERT, A. A. On p-adic fields and rational division algebras. *Ann. Math.* **41** (1940), 674–693.
3. ARTIN, E. AND TATE, J. "Class Field Theory." Harvard Univ. Press, Cambridge, Massachusetts, 1961.
4. DEMUSKIN, S. The group of the maximum p-extension of a local field. (Russian) *Izv. Akad. Nauk. SSSR Ser. Mat.* **25** (1961), 329–346.
5. HALL, M. "The Theory of Groups." Macmillan, New York, 1959.
6. HERSTEIN, I. N. "Theory of Rings." Univ. of Chicago Press, Chicago, Illinois, 1961.
7. SERRE, J.-P. "Cohomologie Galoisienne." Springer, Berlin, 1964.
8. SERRE, J.-P. Corps locaux. *In* Act. Sci. Ind. no. 1296, Hermann, Paris, 1962.
9. SERRE, J.-P. Structure de certains pro-p groupes. Séminaire Bourbaki, exposé 252, 1962–1963.
10. SERRE, J.-P. Théorie des algèbres simples. Séminaire Henri Cartan, no. 6–7, 1950–1951.
11. SHAFAREVIC, I. On p-extensions. (Russian) *Mat. Sb.* **20** (1947), 351–363. (*Am. Math. Soc. Transl.*, Ser. 2, t. 4, 59–72.)
12. WANG, S. On Grunwald's theorem. *Ann. Math.* **51** (1950), 471–484.
13. WEISS, E. "Algebraic Number Theory." McGraw-Hill, New York, 1963.
14. WHAPLES, G. Introduction to class field theory. Lectures at Bowdoin College, summer 1966.